LIBYAN ACADEMY FOR TELECOM AND INFORMATICS

SECURITY + SY601 COURSE MODULE1

Instructor Khaled Gamo

Module1 Attacks, Threats, and Vulnerabilities:

Gamo@HP:~$Whoami

SPEAKERS INFO

MR. KHALED GAMO

Khaled Gamo is managing information Security of Almadar Aljadid, Almadar is first mobile operator in Libya.
He was Director General of National Information Security & Safety Authority (NISSA).
He holds a Bachelor's degree in communication engineering as well as Holding a series of certification in field IT and information security such as CEH, ECSA, CCIE security written exam, CCVP, CCNP, and CCNA.
He has over 18 years of experience in the Telecom Sector and information technology he was working in Huawei Libya as Data communication product manager, also he was technology division manager in Libya post Telecommunication Company.
Khaled was managing cyber security programs at national level including national cyber security strategy and building Libya-CERT. He was also involved in developing Cyber security legislation initiative in Libya.

https://www.facebook.com/carthagearena/videos/1701847216530321/

Course Modules

Attacks, Threats, and Vulnerabilities

Implementation of secure protocol

Architecture and Design

Operations and Incident Response

Governance, Risk, and Compliance

Course Strategy

Having Fun

CTF Scenarios

More & More Practice & Exercises

Explaining subject Practice it

Exercise Every Day as Homework

The global cybersecurity market is set to grow from its current market value of more than $120 billion to over $300 billion by 2024, according to a new research report by Global Market Insights.

The Estimated Annual Cost of Global Cybercrime Is $375 Billion

Yearly Cyber Crime Victim Count Estimates

Victims Per YEAR:

566 Million

Yearly Cyber Crime Victim Count Estimates

Victims Per DAY:

1.5 Million

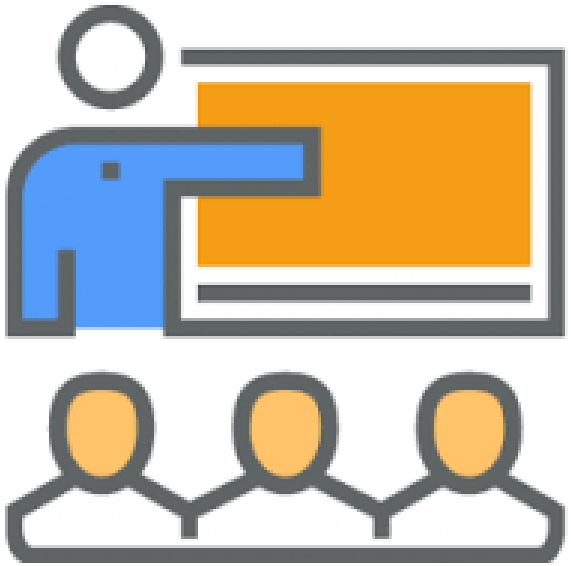
Yearly Cyber Crime Victim Count Estimates

Victims Per SECOND:

18

How Protected Do You Feel?

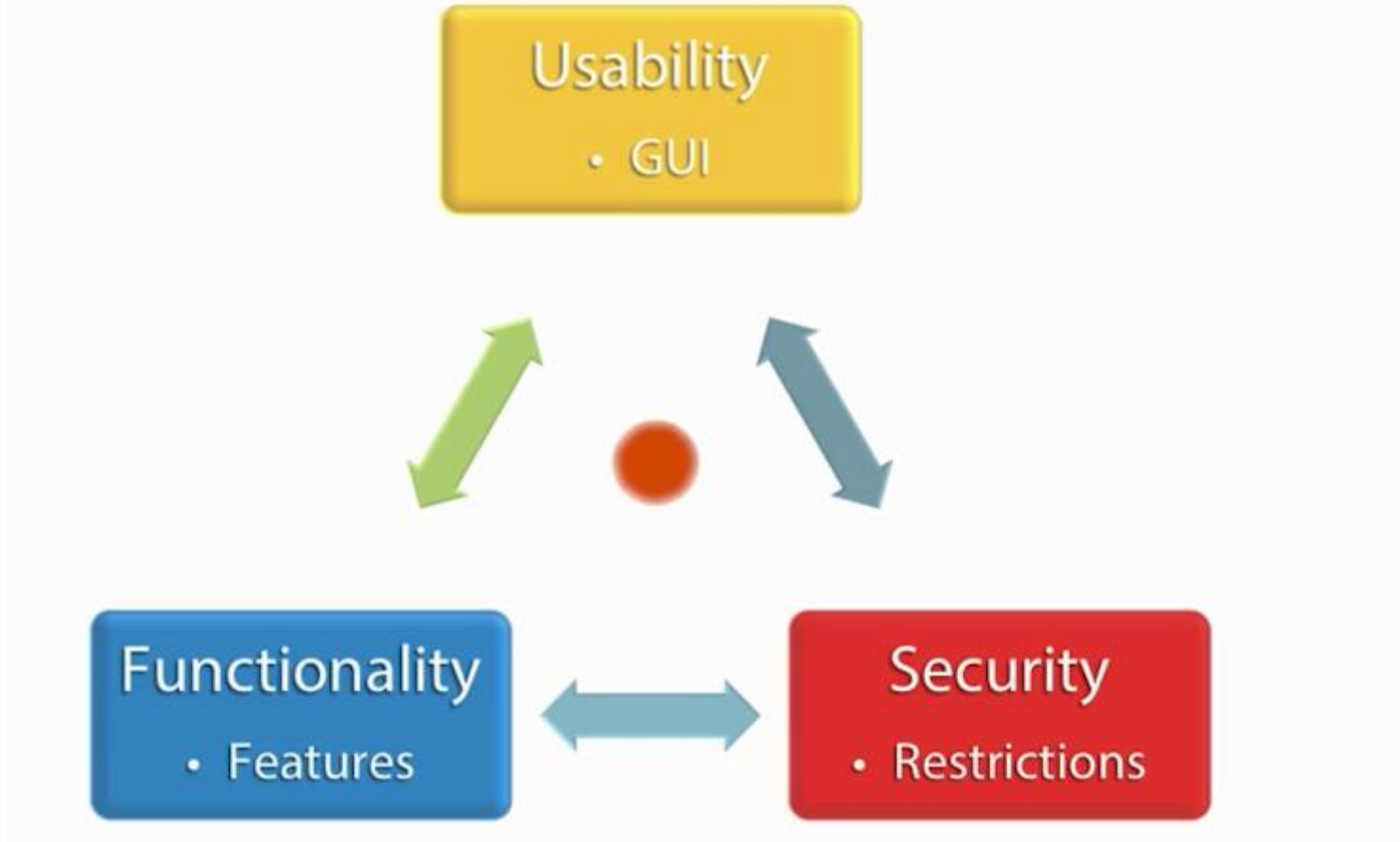
“ Who Should Attend This Course “



- System Administrators
- Security Engineers and consultants
- Network administrators
- IT Auditors/Penetration Testers


CODE OF
ETHICS

The Technology Triangle




1
CONFIDENTIALITY
INFORMATION SECURITY
2
INTEGRITY
3
AVAILABILITY

Vulnerabilities & Controls

a vulnerability is a weakness which can be exploited by an attacker, to perform unauthorized actions within a computer system.

Example of Vulnerabilities

- Default username and password
- Weak password
- No backup policy
- No High Availability

Controls are mechanisms that can reduce the risk of vulnerability been exploited

Threat

A **threat** is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm

Threats exist because of the very existence of the system or activity and not because of any specific weakness

Type	Threats
Physical damage	Fire
	Water damage
Natural events	Volcanic phenomenon
	Flood
Loss of essential services	Failure of air conditioning or water supply system
	Loss of power supply
Disturbance due to radiation	Electromagnetic radiation
	Thermal radiation
Compromise of information	Tampering with hardware
	Theft of media or documents
Technical failures	Equipment failure
	Software malfunction
Unauthorized actions	Unauthorized use of equipment
	Corruption of data
Compromise of functions	Error in use
	Abuse of rights

Relationship: Vulnerability and Threat

Examples

Vulnerabilities	Threats
Warehouse unprotected and without surveillance	Theft
Complicated data processing procedures	Data input error by personnel
No segregation of duties	Fraud, unauthorized use of a system
Unencrypted data	Information theft
Use of pirated software	Lawsuit, virus
No review of access rights	Unauthorized access by persons who have left the organization
No backup procedures	Loss of information

Impact

Examples of impacts on availability	Examples of impacts on confidentiality	Examples of impacts on integrity
• Performance degradation • Service interruption • Unavailability of service • Disruption of operations	• Invasion of privacy of users or customers • Invasion of privacy of employees • Confidential information leakage	• Accidental change • Deliberate change • Incorrect results • Incomplete results • Loss of data

Social Engineering Techniques

Social engineering is a method of using people as part of an attack process.

Social Engineering Methods

Social engineering is an attack against a user, and typically involves some form of social interaction.

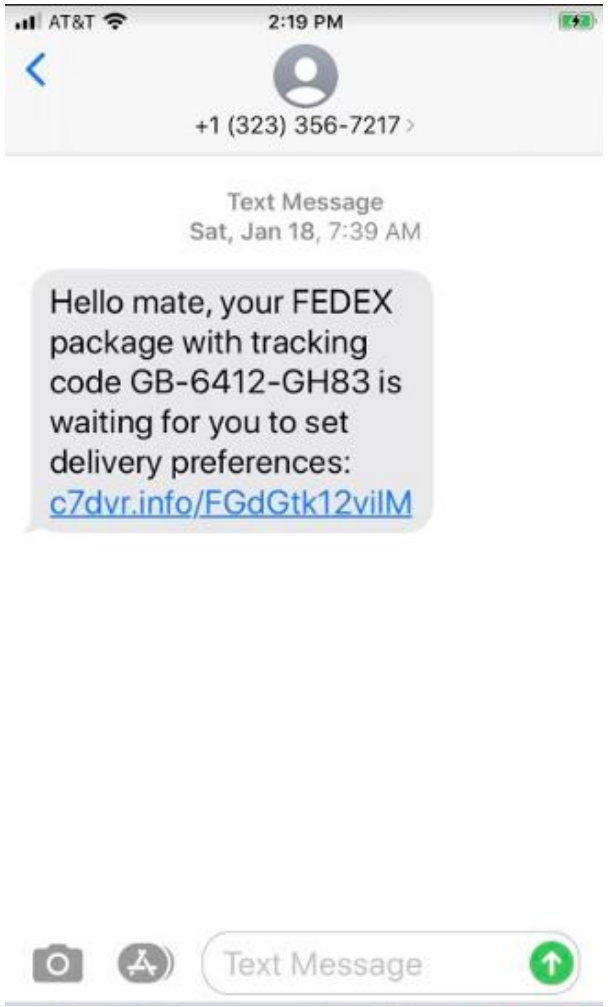
Phishing

is a type of social engineering in which an attacker attempts to obtain sensitive information from users by masquerading as a trusted entity in an e-mail or instant message sent to a large group of often random users.

Social Engineering Methods

Smishing

Smishing is an attack using Short Message Service (SMS) on victims' cell phones. It is a version of phishing via SMS.



Social Engineering Methods

Vishing

- Vishing is a variation of phishing that uses voice communication technology to obtain the information the attacker is seeking.
- Vishing takes advantage of the trust that some people place in the telephone network.
- Users are unaware that attackers can spoof (simulate) calls from legitimate entities using Voice over IP (VoIP) technology.
- Voice messaging can also be compromised and used in these attempts

Social Engineering Methods

Spear Phishing

- Spear phishing is a term created to refer to a phishing attack that targets a specific person or group of people.

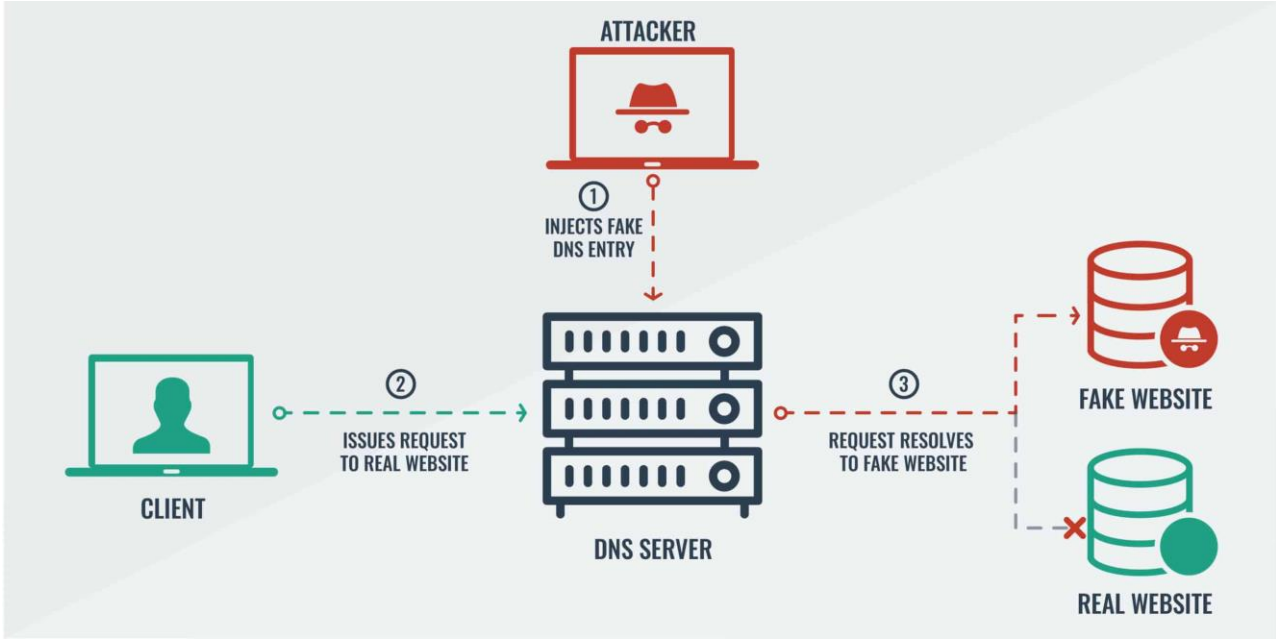
Whaling

- whaling is focused on spear phishing, but specifically at a high-level executive. So, these are your CEOs, your CFOs, your CIOs, your CSOs, or other chief-level executives.

Social Engineering Methods

Pharming

- Pharming the hacker will trick somebody to go to a different website. (usually by modifying hosts file) or by DNS spoofing.



Motivation Factors

Authority. People are much more willing to comply and do what you tell them to if they think it's coming from somebody who's in authority.

Urgency. And urgency is all about the fact that people know that we're in a rush a lot of the time

Scarcity. Now, scarcity is when you use a technique to get people to act quick, much like urgency, but the difference here is that usually, you're going to do it through like an email campaign or phishing, right?

Likability. People want to be and interact with people they like. Social engineers are some of the most friendly and likable people you will ever meet.

Fear, fear is a great motivator if used properly. In fact, ransomware and any virus scans, they live off fear

More Threats

Diversion Theft. Diversion theft occurs when a thief tries to divert a shipment and take responsibility for it, and send it to a different location.

HOAX. hoax is an attempt at deceiving people into believing something is false even if it's true, or making them believe something is true, even if it's false. like a virus hoax. I might send an email out to all of my friends and say, "Hey everybody, there's a virus going around. To protect yourself from it, go to your C drive and delete your boot.ini file

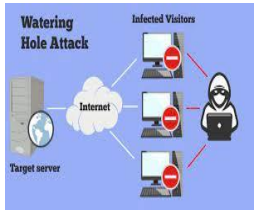
Shoulder Surfing when you're sitting at the office working, and somebody comes up behind you and uses direct observation to obtain authentication information

Eavesdropping is occurs when a hacker intercepts, deletes, or modifies data that is transmitted between two devices

More Threats

Dumpster Diving. This is when a person actually scavenges for personal or confidential information in garbage or recycling containers.

Baiting. is when a malicious individual leaves behind a malware-infected thumb drive or USB drive or a CD someplace around that somebody might have curiosity to pick up and insert into their computer.



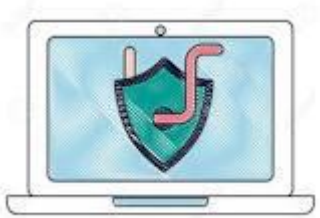
Watering Hole Attack This is when an attacker figures out where your users like to go, like a common website, they attack that website, embed their own malware, so, next time when you go to that website, you download the malware and again, get access.

Type of Attack Indicators

Malware refers to software that has been designed for some nefarious purpose. Such software can be designed to cause damage to a system

Ransomware is a form of malware that performs some action and extracts a ransom from the user. Ransomware typically encrypts files on a system and then leaves them unusable either permanently, acting as a denial of service, or temporarily until a ransom is paid.

A Trojan horse, or simply Trojan, is a piece of software that appears to do one thing (and may, in fact, actually do that thing) but hides some other functionality



Worms are pieces of code that attempt to penetrate networks and computer systems. Once a penetration occurs, the worm will create a new copy of itself on the penetrated system

Type of Attack Indicators

File less viruse, When a piece of malware operates only in memory, never touching the file system, it is much harder to detect. This type of attack is called a fileless virus, or memory-based attack.

Command-and-control servers are used by hackers to control malware that has been launched against targets.

A bot is a functioning piece of software that performs some task, under the control of another program. A series of bots is controlled across the network in a group, and the entire assembly is called a botnet

Spyware is software that “spies” on users, recording and reporting on their activities. Typically installed without the user’s knowledge.

Type of Attack Indicators

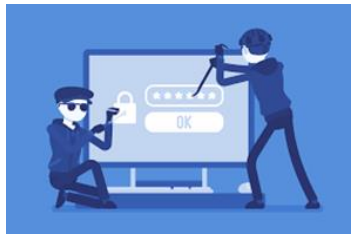
As the name suggests, a key logger is a piece of software that logs all of the keystrokes that a user enters. Key loggers in their own respect are not necessarily evil

A remote-access trojan (RAT) is a toolkit designed to provide the capability of covert surveillance and/or the capability to gain unauthorized access to a target system

Rootkits are a form of malware that is specifically designed to modify the operation of the operating system in some fashion to facilitate nonstandard functionality.

Backdoors were originally (and sometimes still are) nothing more than methods used by software developers to ensure that they can gain access to an application, even if something were to happen in the future to prevent normal access methods.

Type of Attack Indicators Password attack



Password Attack: The most common form of authentication is the user ID and password combination. the combination can be attacked in several ways

Password spraying is an attack that uses a limited number of commonly used passwords and applies them to a large number of accounts

Dictionary Attack: Another method of determining passwords is to use a password-cracking program that uses a list of dictionary words to try to guess the password, hence the name dictionary attack.

Brute Force attack If the user has selected a password that is not found in a dictionary, even if various numbers or special characters are substituted for letters, the only way the password can be cracked is for an attacker to attempt a brute force attack, in which the password-cracking program attempts all possible password combinations.

Type of Attack Indicators Password attack

Offline, brute force attacks can be employed to perform hash comparisons against a stolen password file. This has the challenge of stealing the password file, but if accomplished, it is possible to use high-performance GPU-based parallel machines to try passwords at very high rates and against multiple accounts at the same time.

online When the brute force attack occurs in real time against a system, it is frequently being done to attack a single account with multiple examples of passwords.

Rainbow tables are precomputed tables or hash values associated with passwords. Using rainbow tables can change the search for a password from a computational problem to a lookup problem.

Passwords that are stored are subject to retrieval. Any time a system can send you a copy of your password, there is a security issue. **Plaintext password attacks** are those taken against these specific issues.

Type of Attack Indicators Physical Attacks

Malicious Universal Serial Bus (USB) Cable

Most users view a USB cable as just a wire, but in fact a USB cable can have embedded electronics in it. “Poisoned” cables have been found with electronics that can deliver malware to machines

Malicious Flash Drives

Malicious USB storage devices have been around for a long time. They have been used to dupe users into picking them up, plugging them into their machine, and accessing an attractive folder

Card Cloning

Should someone get physical possession of your credit card, it is possible to copy the information on the magnetic strip, enabling the person to later make a clone of your card

Skimming

Skimming devices are physical devices built to intercept a credit card. These devices are placed on credit card readers to skim the data from the card while passing it on to the legitimate reader.

Type of Attack Indicators AI

Adversarial Artificial Intelligence (AI)

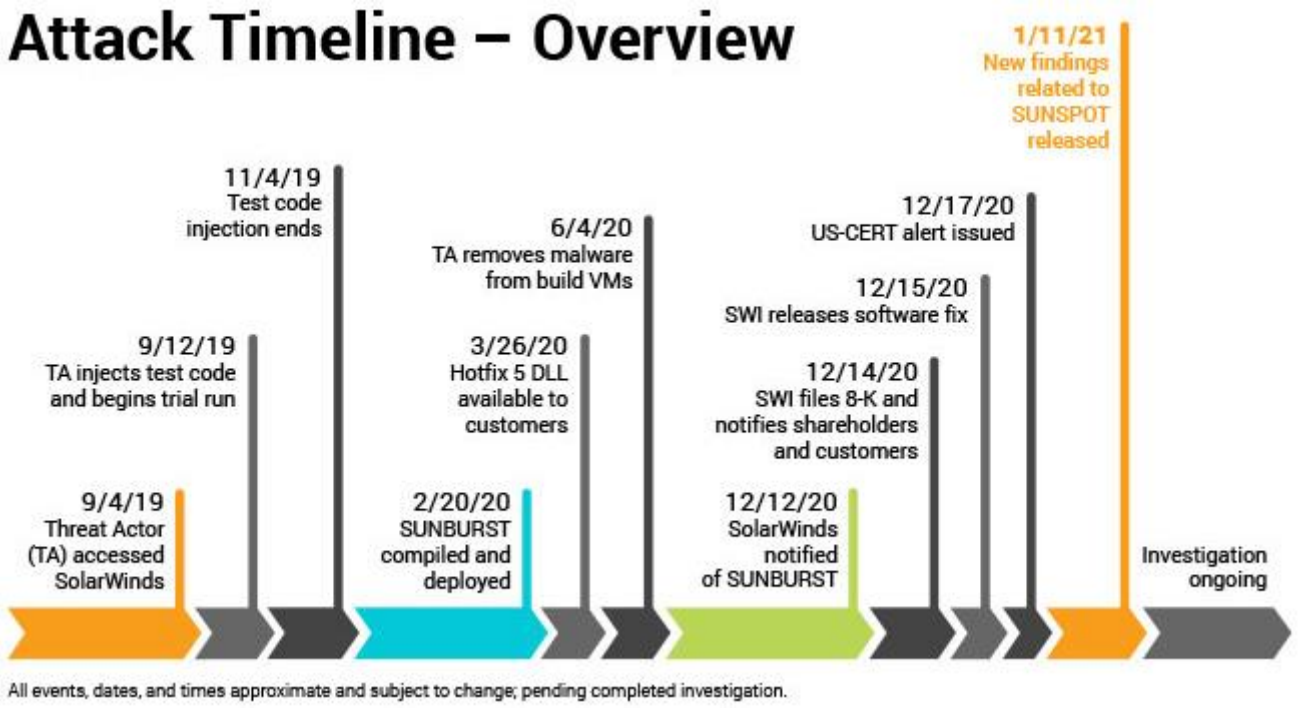
AI brings power to computer solutions because AI models can analyze more combinations of inputs than a human, and do so faster and with more accuracy. AI-enabled systems are used in anti-malware products to find new threats based on analytical analysis of programmatic behaviors. Can AI also be used to evade defenses?

Tainted Training Data for Machine Learning (ML)

Machine learning (ML) is one of the techniques used in AI. ML works by using a training data set to calibrate the detection model to enable detection on sample data.

Supply-Chain Attacks

A supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.



SolarWinds attack highlights supply chain risk

Cloud-Based vs. On-Premises Attacks

- Using cloud computing to improve security only works if you choose a cloud vendor with a security solution as part of the package.
- not all vendors have the same level of protection.
- Moving computing or storage to the cloud, in itself, does not change the security equation.
- Cloud computing is merely using someone else's resources, and you get what you pay for, as in all contracts.
- Whether you are doing security in house against in-house systems or against cloud-based systems, the objectives and methods are the same.

Cryptographic Attacks

- Attacks against the cryptographic system are referred to as cryptographic attacks.
- These attacks are designed to take advantage of two specific weaknesses.
- First, users widely view cryptography as “magic,” or otherwise incomprehensible stuff, leading them to trust the results without valid reasons.
- Second, weaknesses that can be exploited are frequently overlooked by developers.

Application Attack Indicators

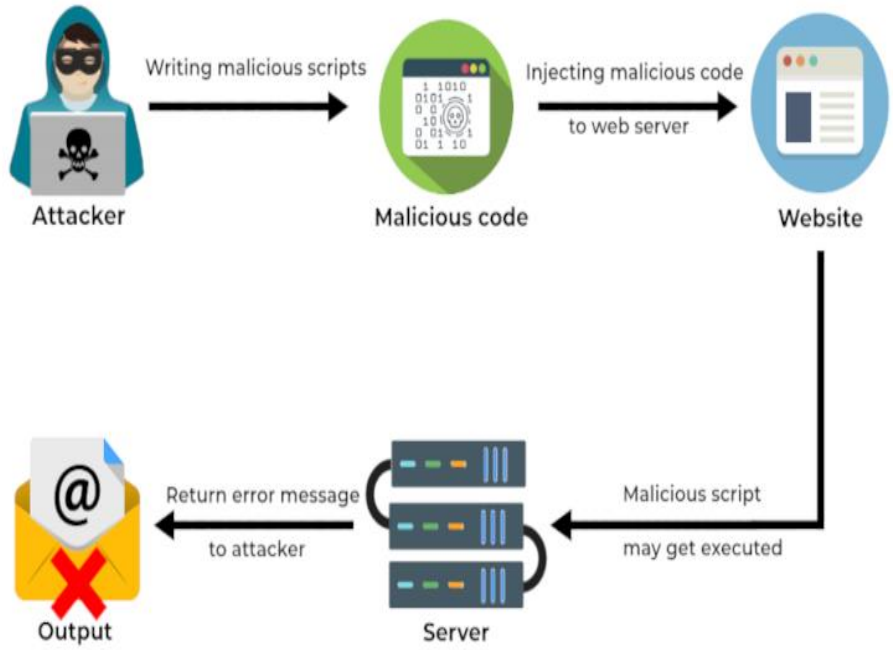
Directory Traversal

- A directory traversal, which is going to exploit insecurely-coded web applications and servers. A directory traversal is a method of accessing unauthorized directories by moving through the directory structure on a remote server.

Application Attack Indicators

Remote code execution

- A remote code execution occurs when the attacker is able to execute or run commands on a remote computer. Notice the key difference here between an arbitrary and a remote code execution. With a remote code execution, the attacker can run the commands remotely, such as through an interactive shell session or some other kind of attack.

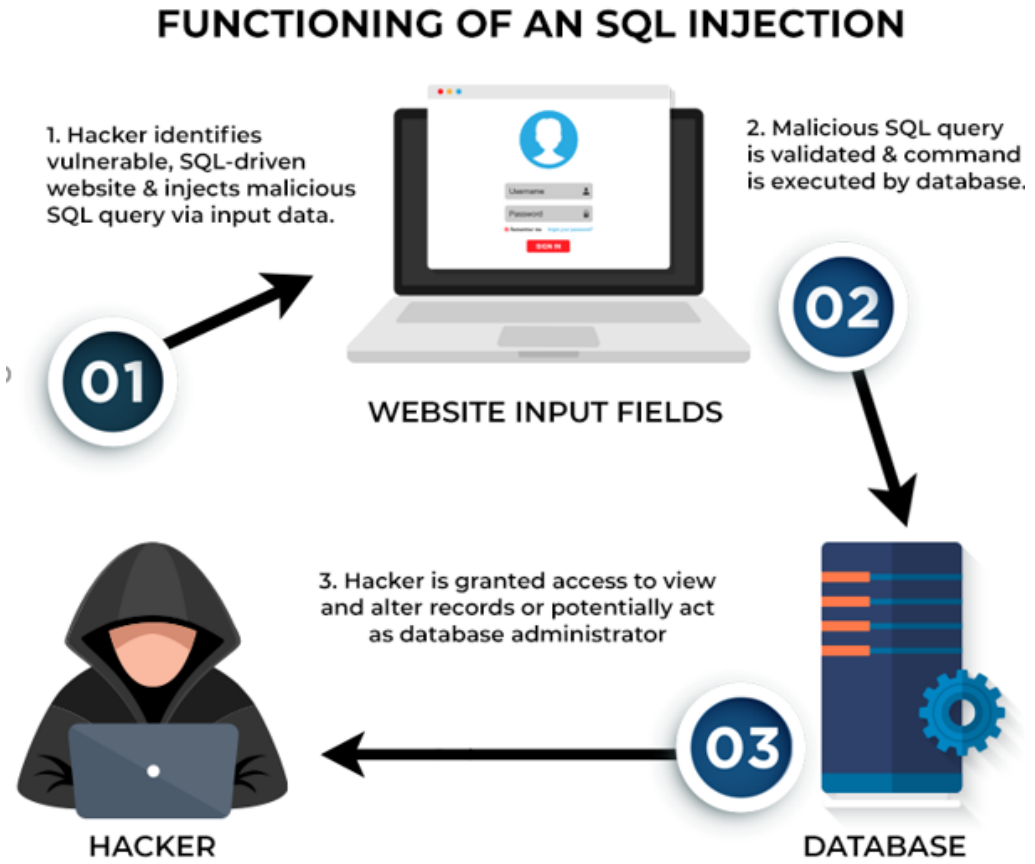


Application Attack Indicators

SQL Injection Attacks

- User input without input validation results in an opportunity for an attacker to craft input to create specific events that occur when the input is parsed and used by an application. Structured Query Language **(SQL) injection**

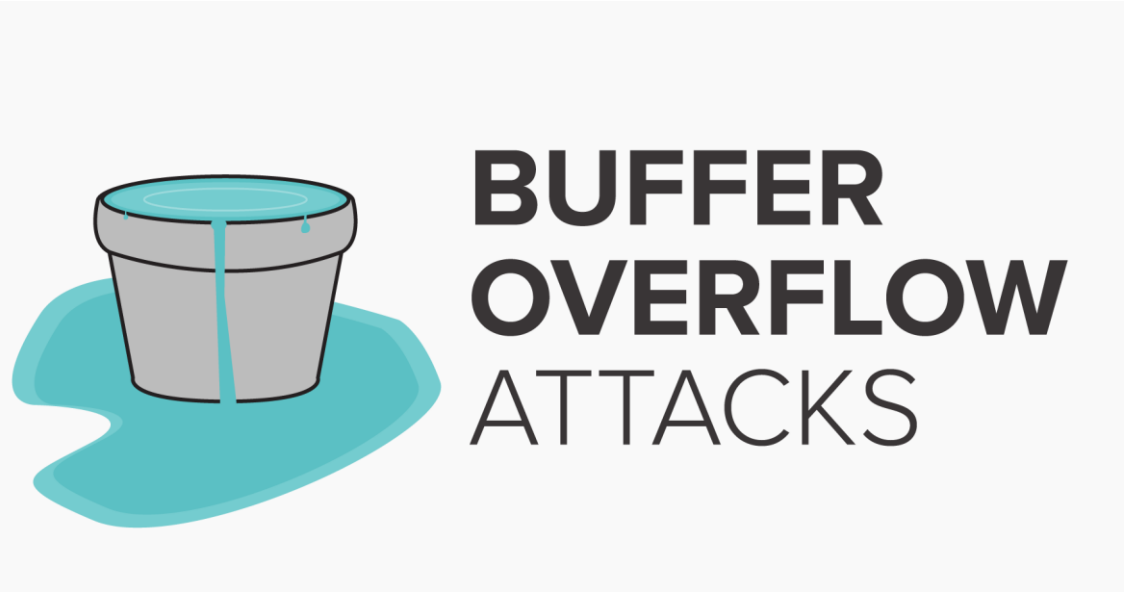
- attacks involve the manipulation of input, resulting in a SQL statement that is different from the statement the designer intended.



Application Attack Indicators

Buffer Overflow

The concept behind these vulnerabilities is relatively simple. The input buffer that is used to hold program input is overwritten with data that is larger than the buffer can hold. The root cause of this vulnerability is a mixture of two things: poor programming practice and programming language weaknesses



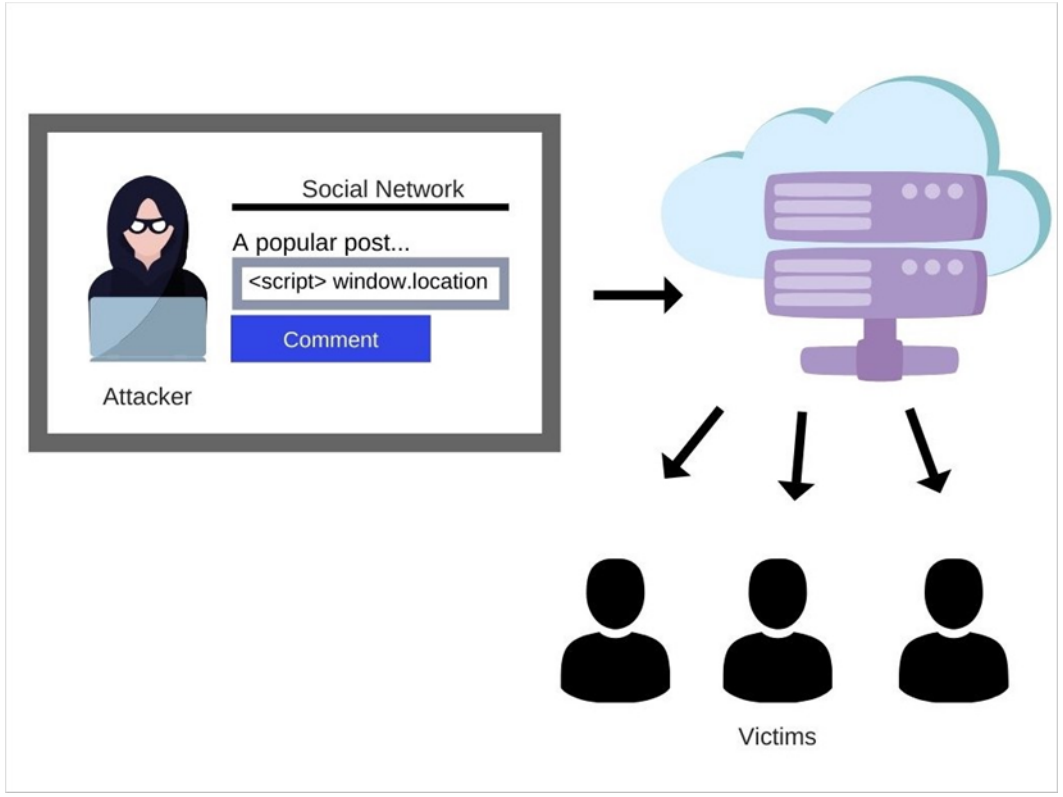
Application Attack Indicators

XSS & XSRF

Cross-site scripting occurs when an attacker embeds malicious scripting commands into a trusted website. When this occurs, the attacker is trying to gain elevated privileges, steal information from the victims cookies, or gain other information stored by the victim's web browser. During a cross-site scripting attack, the victim is the user, not the web server. The web server has already been compromised, possibly.

There are three types of cross-site scripting attacks:

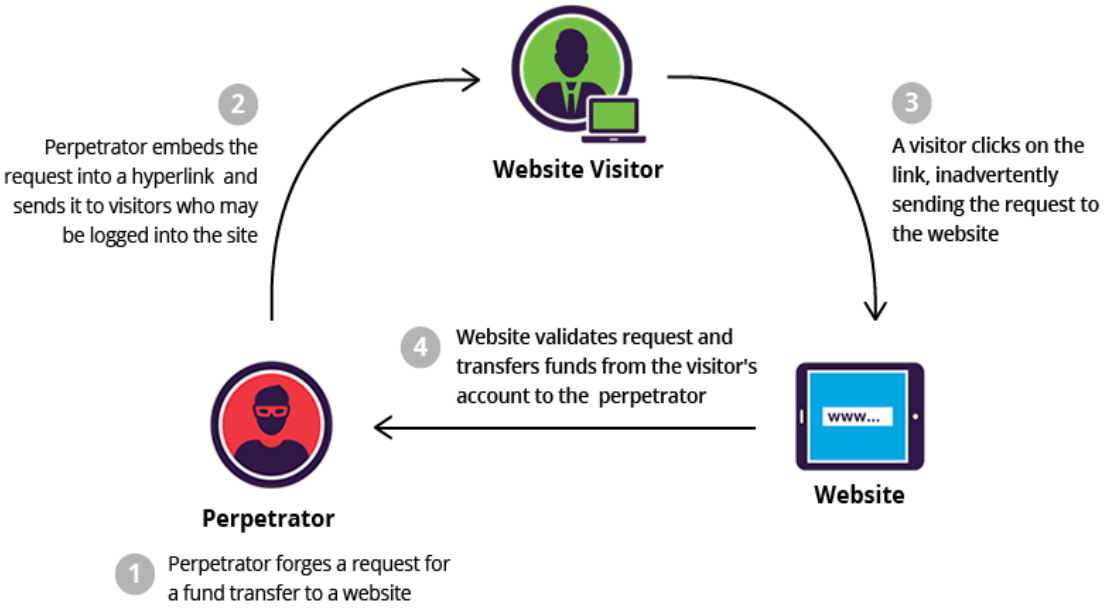
- Stored and persistent
- Reflected
- DOM-based attacks



Application Attack Indicators

XSS & XSRF

In a cross-site request forgery, the attacker forces the user to execute actions on a web server that they already have been authenticated to. For example, let's say that you've already logged into your bank's website and provided your username and your password. At this point, you're already authenticated and the website trusts you. If an attacker can send a command to the web server through your authenticating session, they are forging the request to make it look like it came from you.



Application Attack Indicators

Zero-day exploit

This is an attack against a vulnerability that is unknown to the original developer or manufacturer. Because of this, zero-day vulnerabilities have become a big business, with some companies paying thousands of dollars to penetration testers who can help to identify these vulnerabilities and report them under their bug bounty programs.

Application Attack Indicators

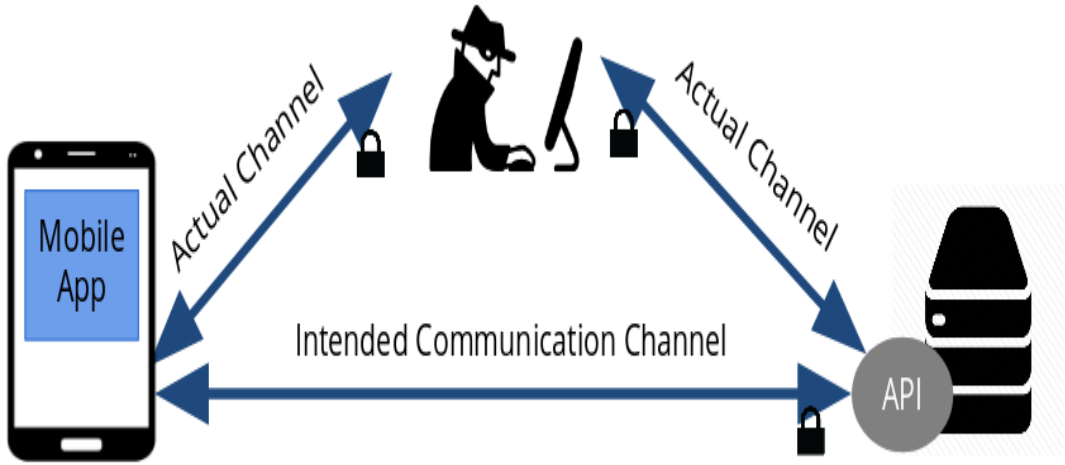
Improper Input Handling

Improper input handling or input validation is the root cause behind most overflows, injection attacks, and canonical structure errors.
Users have the ability to manipulate input, so it is up to the developer to
handle the input appropriately to prevent malicious entries from having an
effect.

Application Attack Indicators

Application Programming Interface (API) Attacks

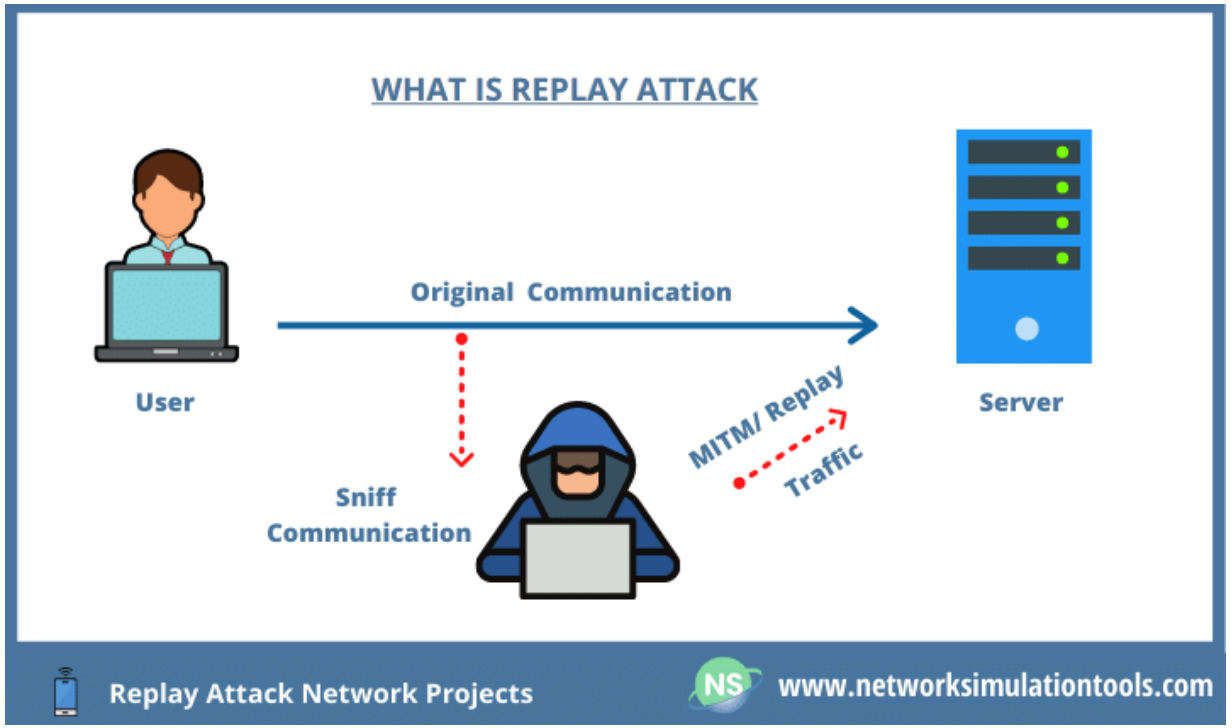
An application (or app) typically interfaces with the service via an application programming interface (API). As with all entry points, APIs are subject to attack and abuse.
An application programming interface attack is one where an attacker specifically attacks the API and the service behind it by manipulating inputs.



Application Attack Indicators

Replay Attacks

If an attacker can record a series of packets and then replay them, what was valid before may well be valid again. An example of this would be repeating the
previous set of transactions, like getting paid twice or successfully passing a security check at a login event.



Application Attack Indicators

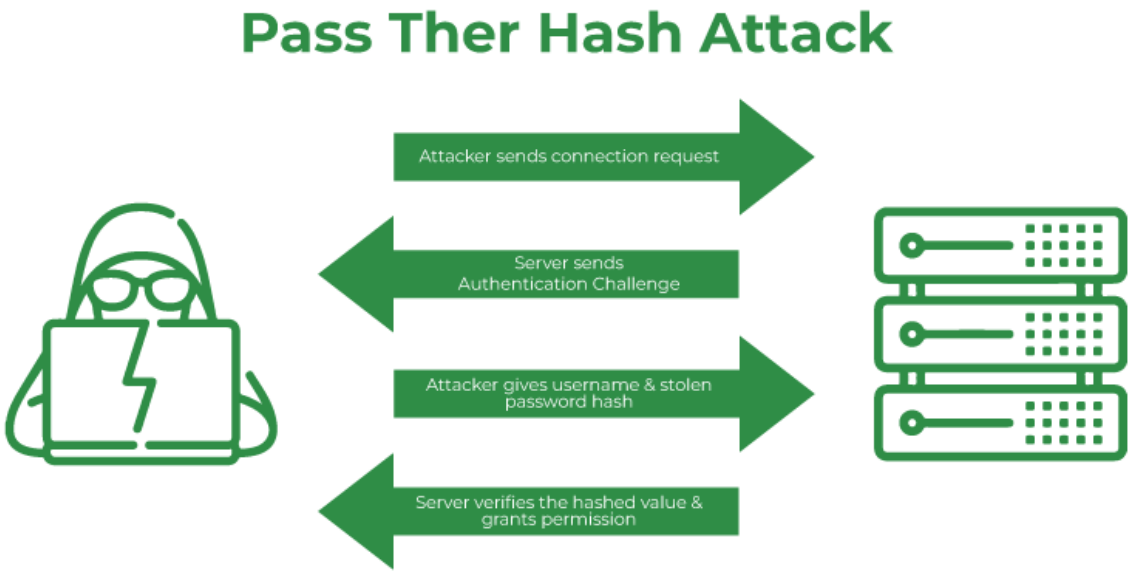
Shimming Attacks

Shimming is a process of putting a layer of code between the driver and the OS. Shimming allows flexibility and portability by enabling changes between different versions of an OS without modifying the original driver code.

Application Attack Indicators

Pass The Hash Attacks

Pass the hash is a hacking technique where the attacker captures the hash used to authenticate a process. They can then use this hash by injecting it into a process in place of the password. This is a highly technical attack that targets the Windows authentication process by injecting a copy of the password hash directly into the system.

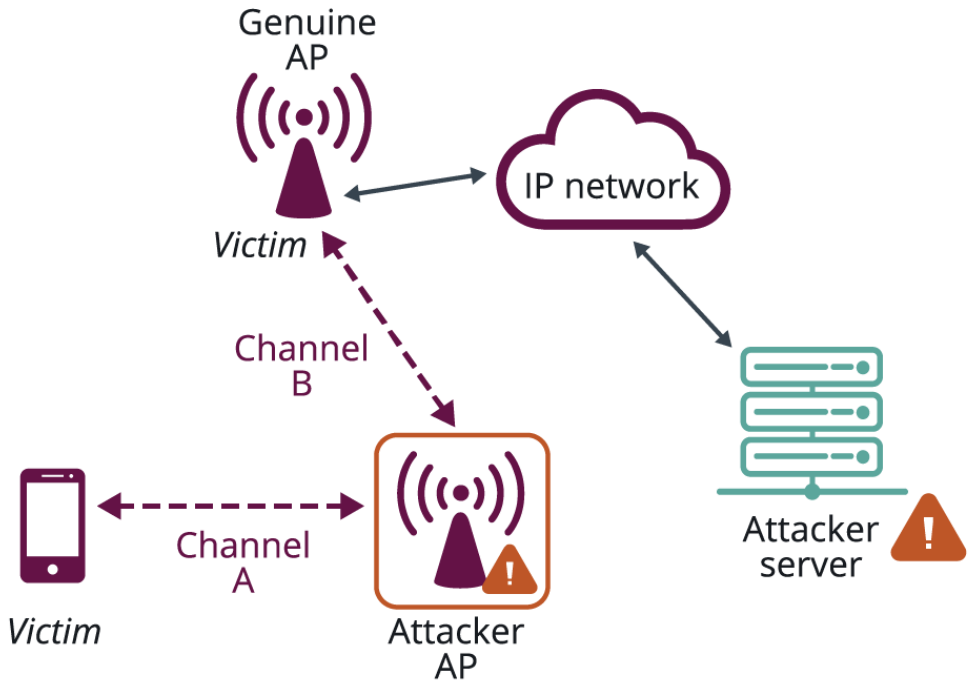


Network Attack Indicators

Network Attack Indicators

Evil Twin Attack

- The evil twin attack is an attack against the wireless protocol via substitute hardware.
- This attack uses an access point (AP) owned by an attacker that usually has been enhanced with higher-power and higher-gain antennas to look like a better connection to the users and computers attaching to it.
- By getting users to connect through the “evil” access point, attackers can more easily analyze traffic and perform man in the middle−type attacks.
- For simple denial of service (DoS), an attacker could use interference to jam the wireless signal, not allowing any computer to connect to the access point successfully



Network Attack Indicators

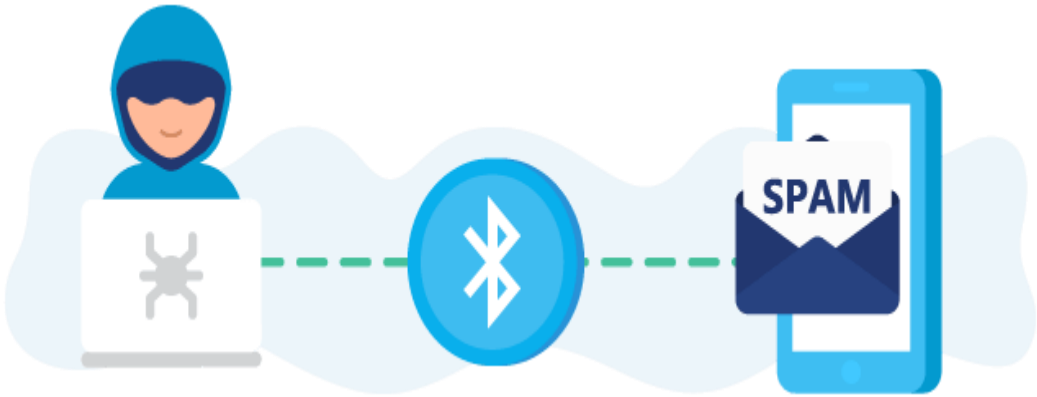
Rogue Access Point

- By setting up a rogue access point, an attacker can attempt to get clients to connect to it as if it were authorized and then simply authenticate to the real
- AP—a simple way to have access to the network and the client's credentials.
- Rogue APs can act as a man in the middle and easily steal users' credentials.
- Enterprises with wireless APs should routinely scan for and remove rogue APs, as users have difficulty avoiding them.

Network Attack Indicators

Bluejacking attack

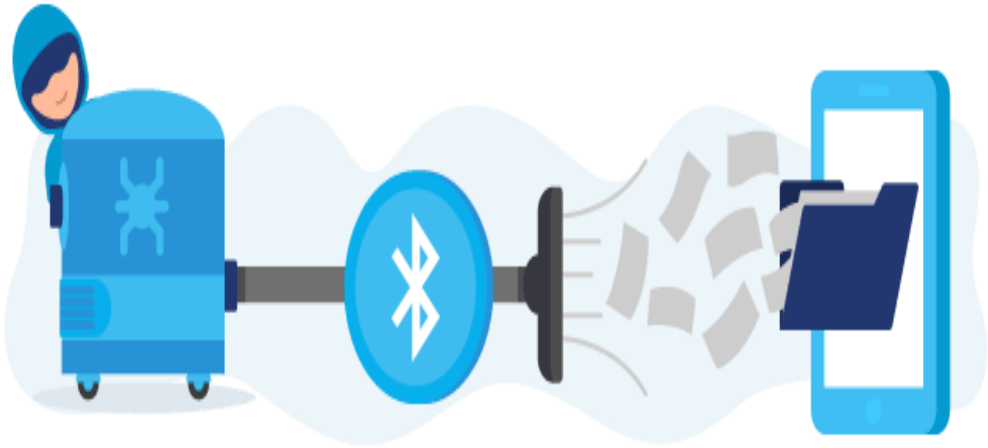
This type of cyber attack involves one Bluetooth-enabled device hijacking another and sending spam messages to the hijacked device.



Network Attack Indicators

Bluesnarfing attack

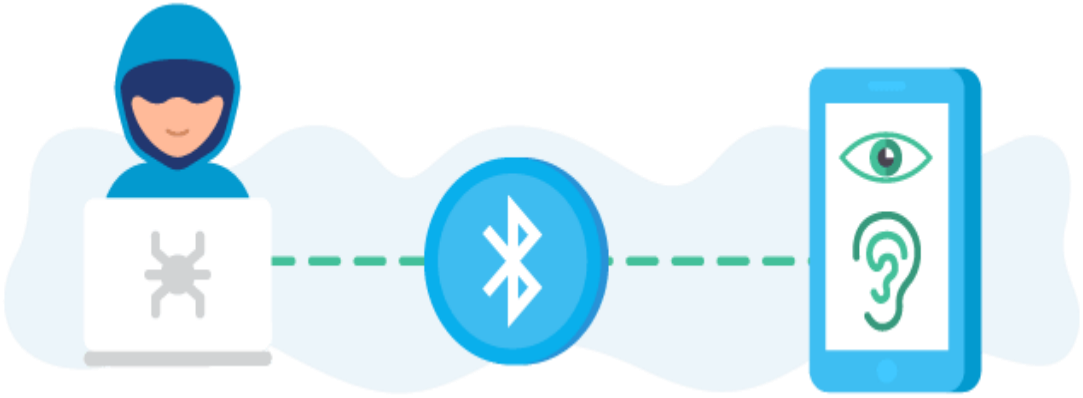
A bluesnarfing attack is similar to bluejacking, but more sinister. Where bluejacking only sends information to your device, bluesnarfing also extracts information from your device. Data like text messages, photos, emails, and even the identifying information your device sends to your ISP can all be stolen. The hacker can use this information for a variety of purposes, none of them good.



Network Attack Indicators

Bluebugging attack

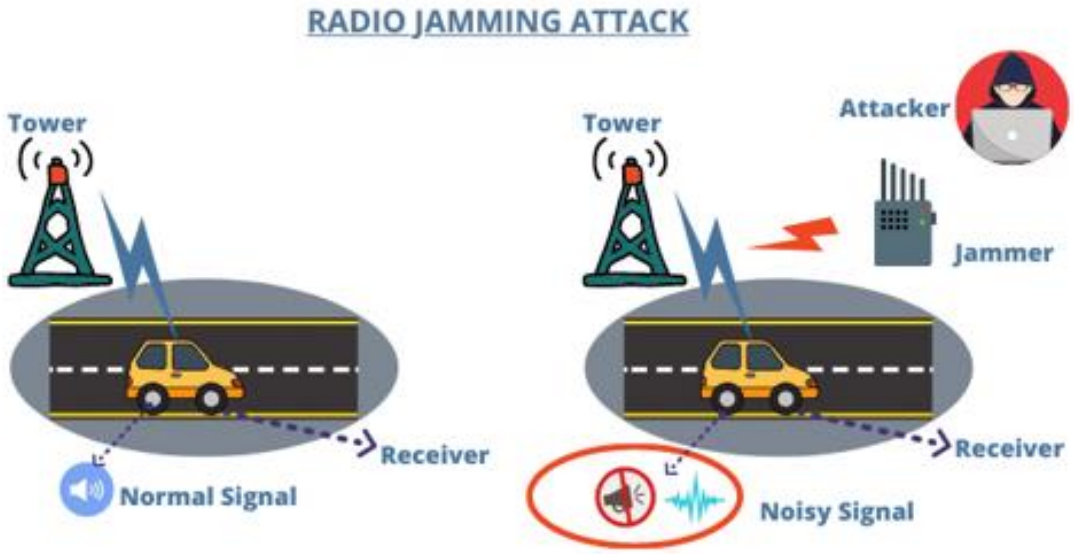
Here, hackers establish a surreptitious Bluetooth connection with your phone or laptop. They then use this connection to gain backdoor access to your device. Once in, they can spy on your activity, access your sensitive information, and even use your device to impersonate you on any apps on your device, including the apps you use for online banking.



Network Attack Indicators

Jamming attack

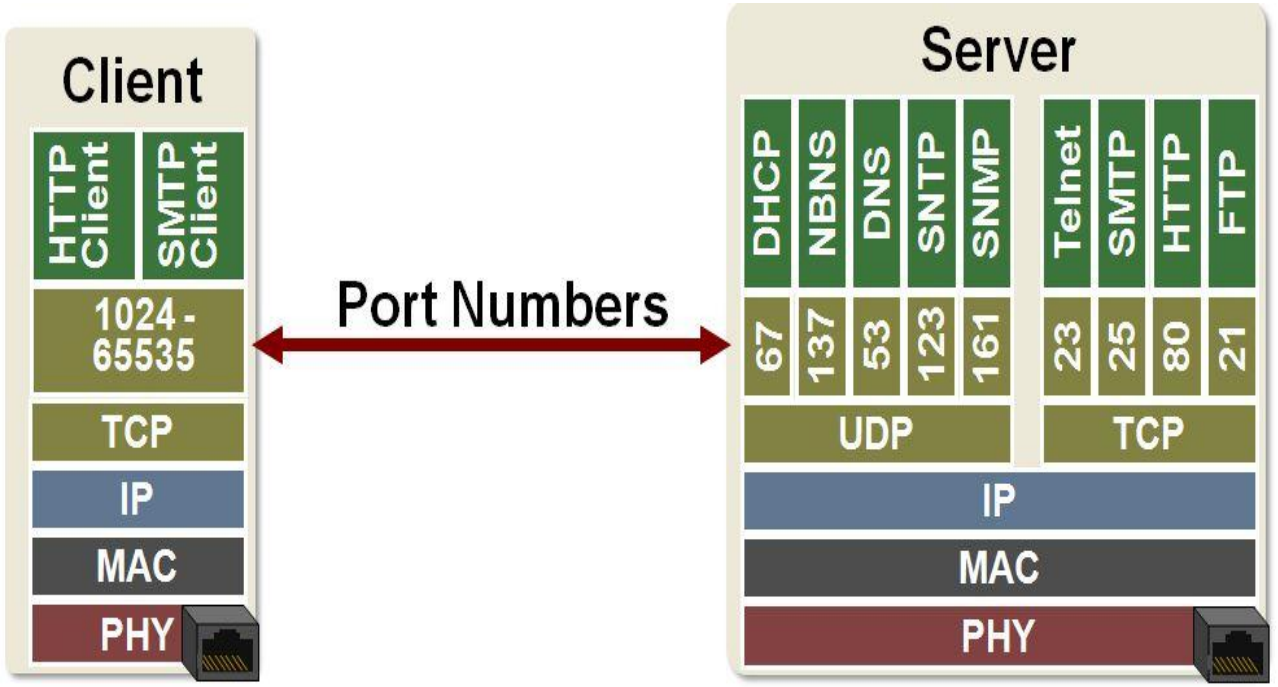
Jamming is a form of denial of service that specifically targets the radio spectrum aspect of wireless. Just as other DoS attacks can manipulate things behind the scenes, so can jamming on a wireless AP, enabling actions such as attaching to a rogue AP



Network Attack Indicators

Unnecessary ports

an unnecessary port is simply one that's associated with a service or a function that you don't need or is considered non-essential. For example, if you have a server whose entire function is to act as a mail relay server, all it's designed to do is send mail out, then the only thing it needs is a couple of ports open. It needs port 25 for SMTP and port 465 or 587 for SMTP over SSL and TLS.

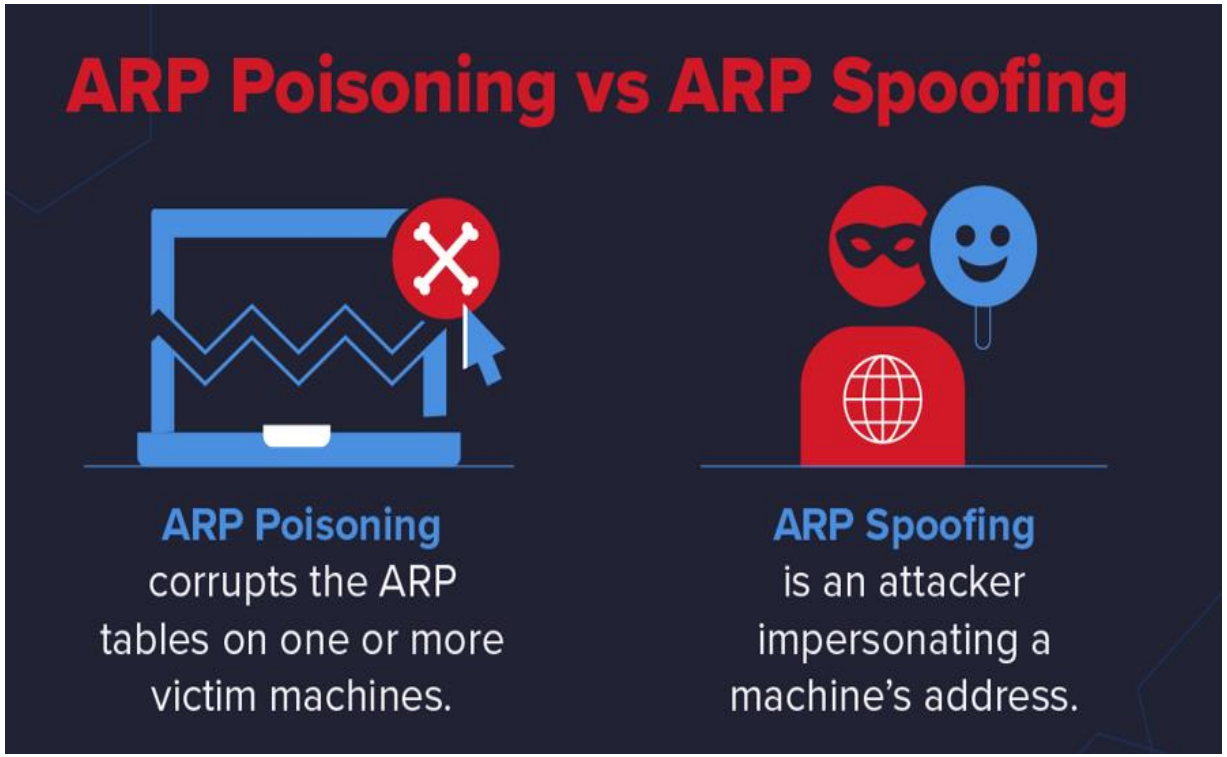


Network Attack Indicators

Layer 2 Attacks

(ARP) Poisoning & ARP Spoofing

There is no mechanism to verify the veracity of the data received. An attacker can send messages, corrupt the ARP table, and cause packets to be misrouted. This form of attack is called ARP poisoning and results in malicious address redirection.

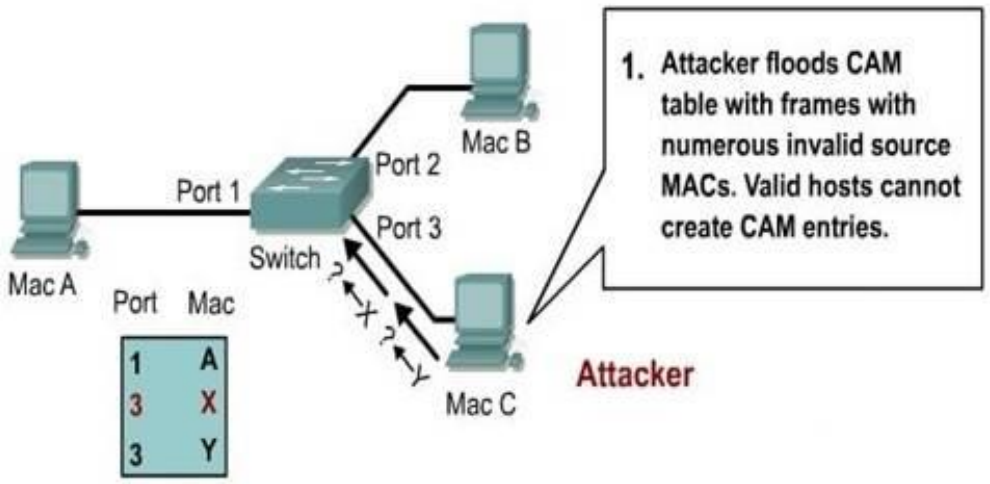


Network Attack Indicators

Layer 2 Attacks

(MAC) Flooding

MAC flooding is an attack where an attacker floods the table with addresses, making the switch unable to find the correct address for a packet. The switch responds by sending the packet to all addresses, in essence acting as a hub.

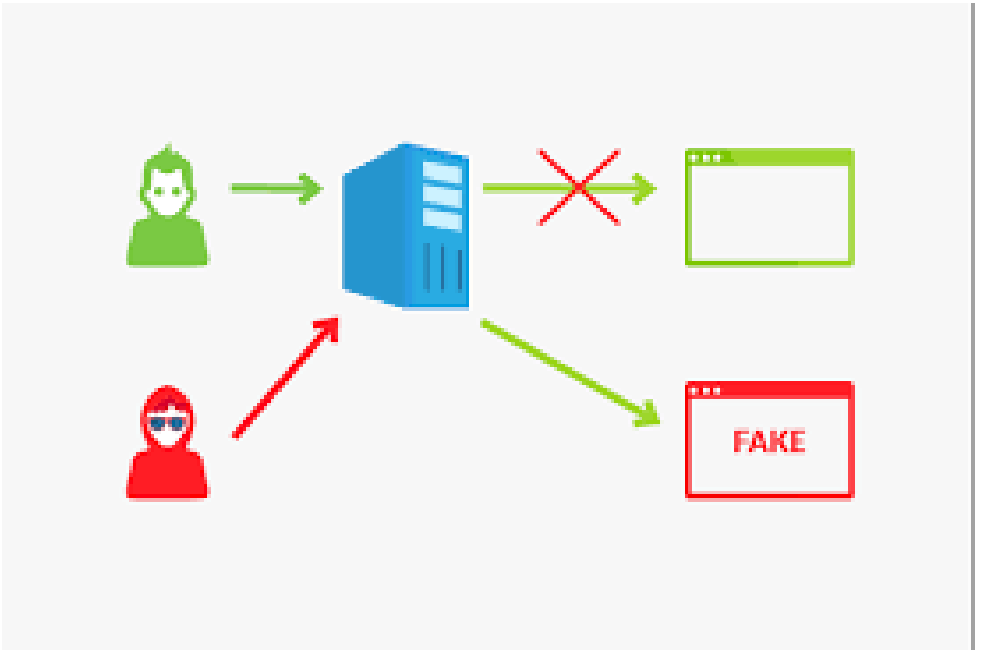


Network Attack Indicators

DNS attacks

Domain Hijacking

Domain hijacking is the act of changing the registration of a domain name without the permission of its original registrant. Technically a crime, this act can have devastating consequences because the DNS system will spread the false domain location far and wide automatically. The original owner can request it to be corrected, but this can take time.

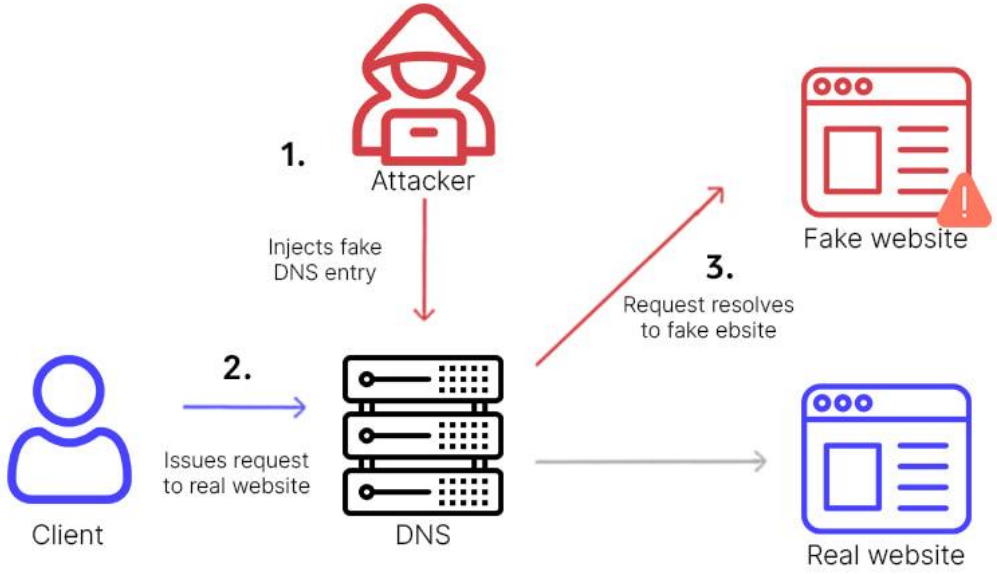


Network Attack Indicators

DNS attacks

DNS Poisoning

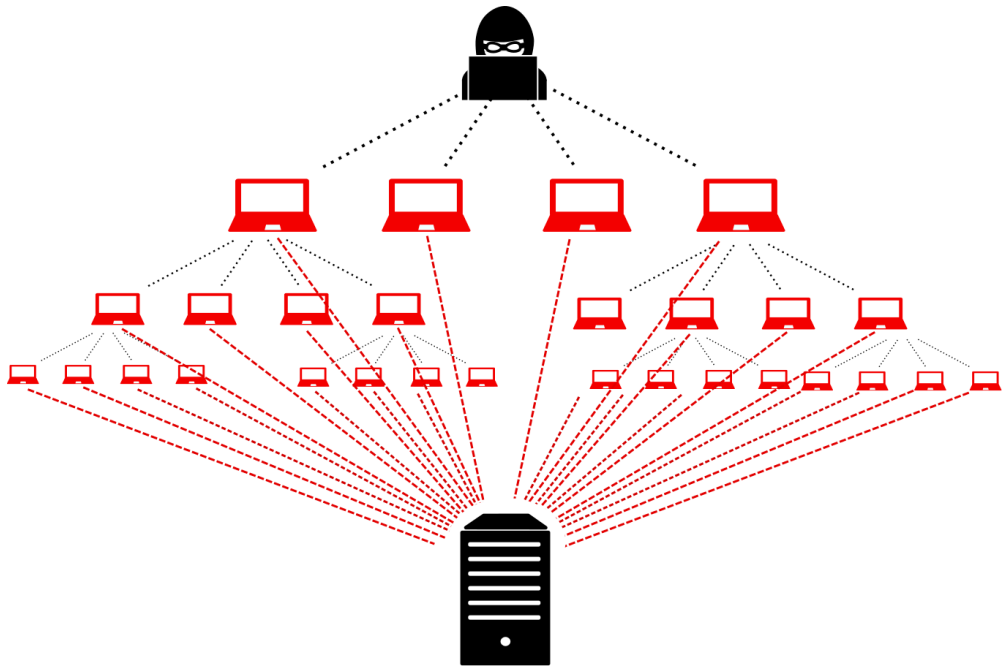
DNS poisoning is a variant of a larger attack class referred to as DNS spoofing. In DNS spoofing, an attacker changes a DNS record through any of a multitude of means. There are many ways to perform DNS spoofing, a few of which include compromising a DNS server, the use of a false network node advertising a false DNS address. An attacker can even use DNS cache poisoning to result in DNS spoofing.
By poisoning an upstream DNS cache, all of the downstream users will get spoofed DNS records.



Network Attack Indicators

Distributed Denial-of-Service (DDoS) attack

In a denial-of-service (DoS) attack, the attacker attempts to deny authorized users access either to specific information or to the computer system or network itself. This can be accomplished by crashing the system—taking it offline—or by sending so many requests that the machine is overwhelmed. A DoS attack employing multiple attacking systems is known as a distributed denial-of-service (DDoS) attack. The goal of a DDoS attack is also to deny the use of or access to a specific service or system. DDoS attacks were made famous in 2000 with the highly publicized attacks on eBay, CNN, Amazon, and Yahoo!



Threat Actors, Vectors, and Intelligence Sources

Security Threats

Hosts


Footprinting
Physical Security
windows8user
Locked
Password
Windows 8
Passwords
Malware

Hosts


Denial of Service


Unauthorized
Access


Privilege Escalation


Back Doors


Natural
Earthquakes
Hurricanes
Floods
Natural Disasters

Physical

Theft

Impact

Power

End of Life

Applications

Configuration

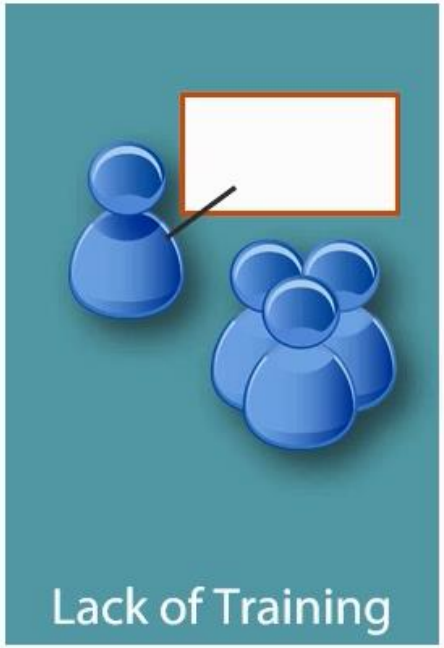
Buffer Overflow

Lazy Coding

Data/Input Validation

Human


Malicious
Employees


Lack of Training


Social Networking


Hackers

Network

Where Do Most Attacks Come From?

External | Foreign Countries | Internal

Hacking Concepts

Hacking is exploiting security controls either in a technical, physical or a human-based element

— **Kevin Mitnick**

Who? What? Where?

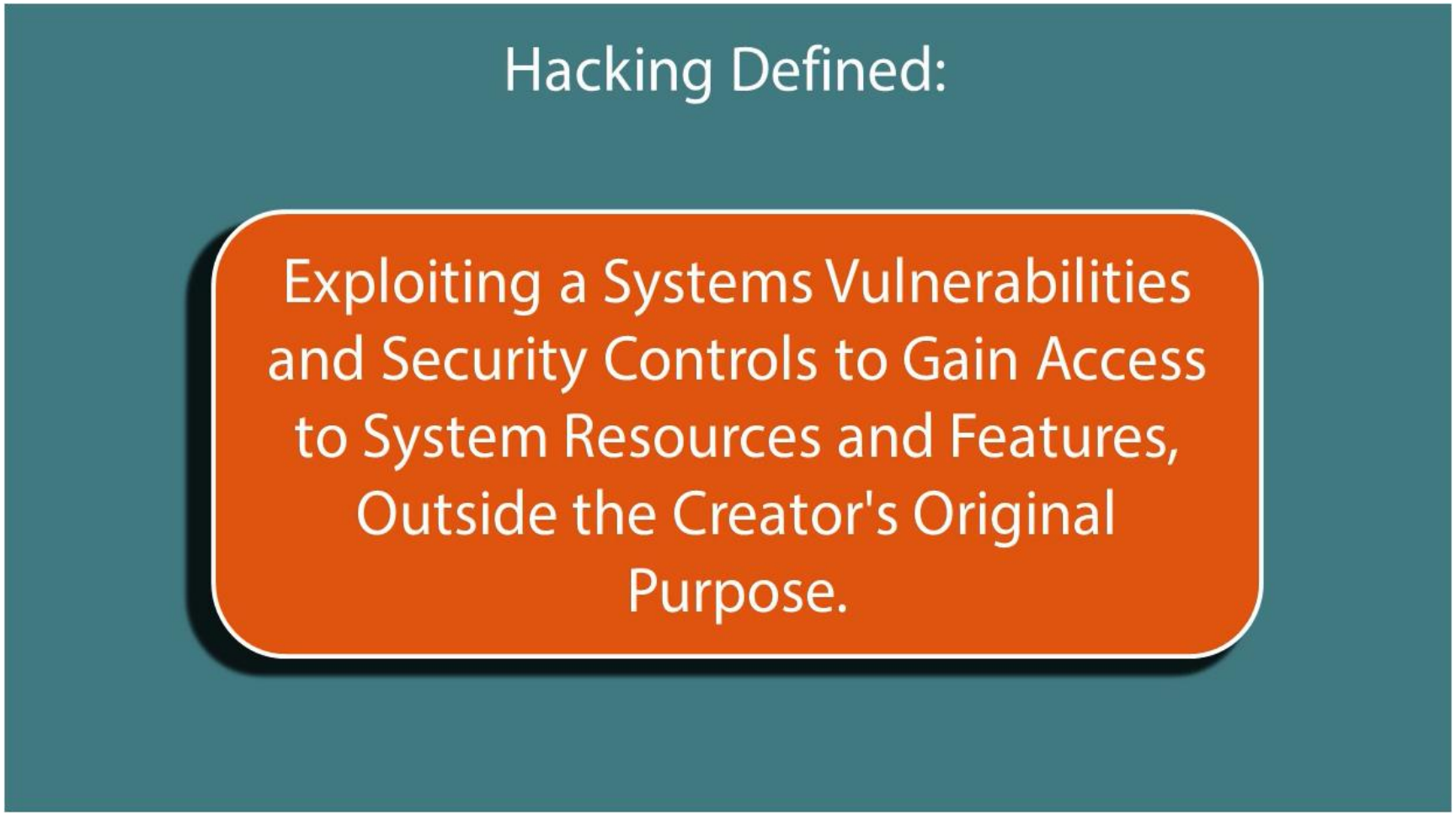
What is hacking?

What's an Ethical Hacker?

Types of hackers?

Why do they hack?

How does hacking influence companies?


Hacking Defined:
Exploiting a Systems Vulnerabilities and Security Controls to Gain Access to System Resources and Features, Outside the Creator's Original Purpose.

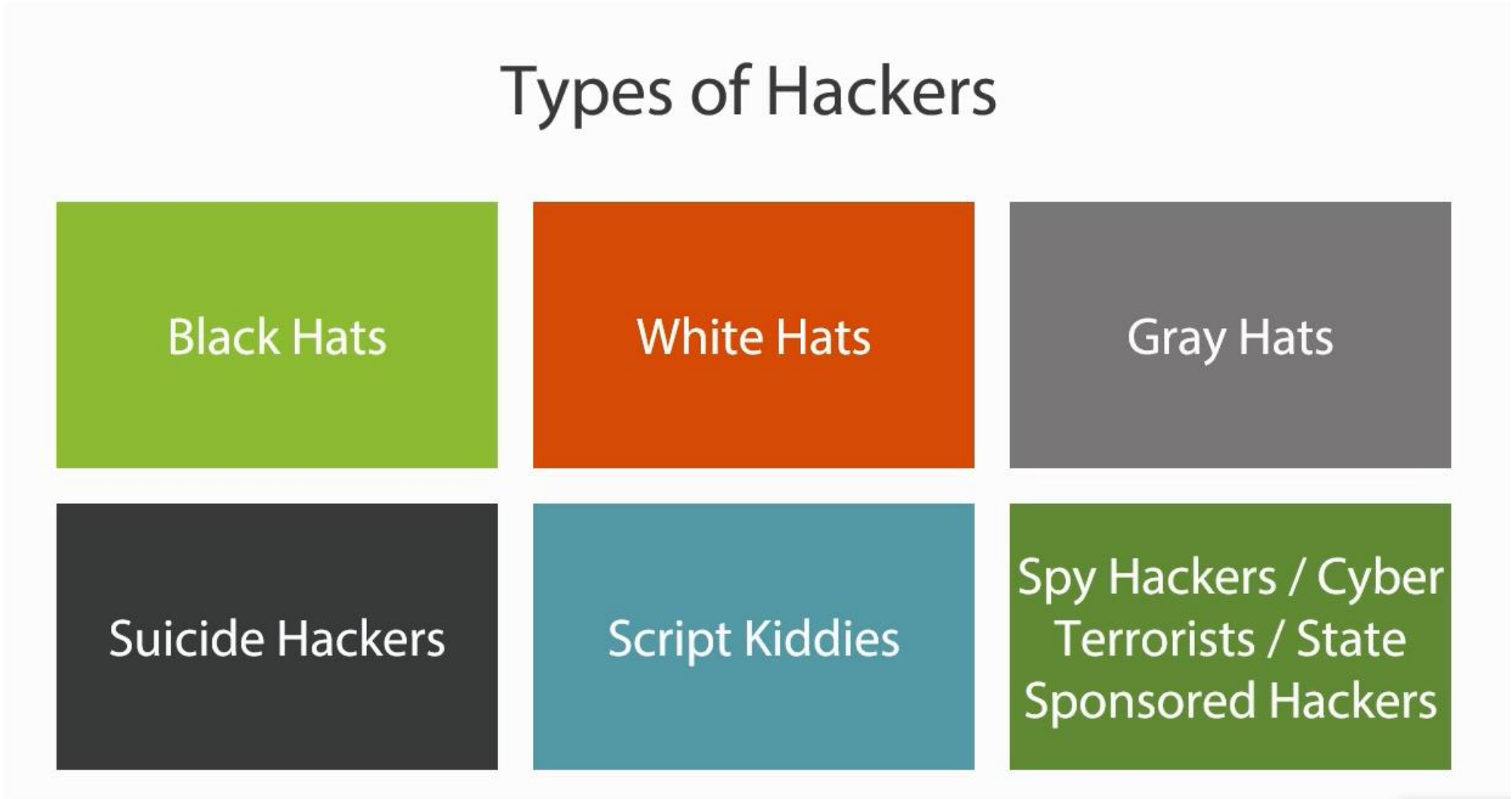
Why a Hacker Hacks

Hobby

Illegal Activities

Malicious Intent

Gain Knowledge


Types of Hackers
Black Hats
White Hats
Gray Hats
Suicide Hackers
Script Kiddies
Spy Hackers / Cyber Terrorists / State Sponsored Hackers

Open Source Intelligence (OSINT)

sometimes called open source threat intelligence, refers to intelligence data collected from public sources. There is a wide range of public sources of information concerning current cybersecurity activity

- Department of Homeland Security (DHS)
- Federal Bureau of Investigation (FBI) investigations.
- SANS Internet Storm Center
- Virus Total.
- Cisco The Talos Intelligence team.
- Cyber security Vendors
- Alien vault otx
- openCTI

https://otx.alienvault.com/dashboard/new

Open Source Intelligence (OSINT)

Vulnerability Databases

Vulnerabilities are the weaknesses in software that allow an attacker a means of entry. You need to know what is vulnerable and either patch the vulnerability or provide a defensive solution to prevent the vulnerability from being exposed to an attacker.

- National Vulnerability Database (NVD)
- Exploit-DB
- Common Vulnerability exposure

Open Source Intelligence (OSINT)

Public/Private Information Sharing Centers

public/private information sharing centers are Information Sharing and Analysis Centers (ISACs) and Information Sharing And analysis Organizations (ISAOs). ISAOs vary greatly in capability but essentially include any organization, whether an industry sector or geographic region, that is sharing cyber-related information for the purpose of enhancing their members' cybersecurity posture

Open Source Intelligence (OSINT)

Dark Web

The dark web is a subset of the worldwide content on the Internet that has its access restricted via specific obfuscation methods. Dark web sites are sites that require Tor—a free, open source software that enables anonymous communication.

Open Source Intelligence (OSINT)

Indicators of Compromise

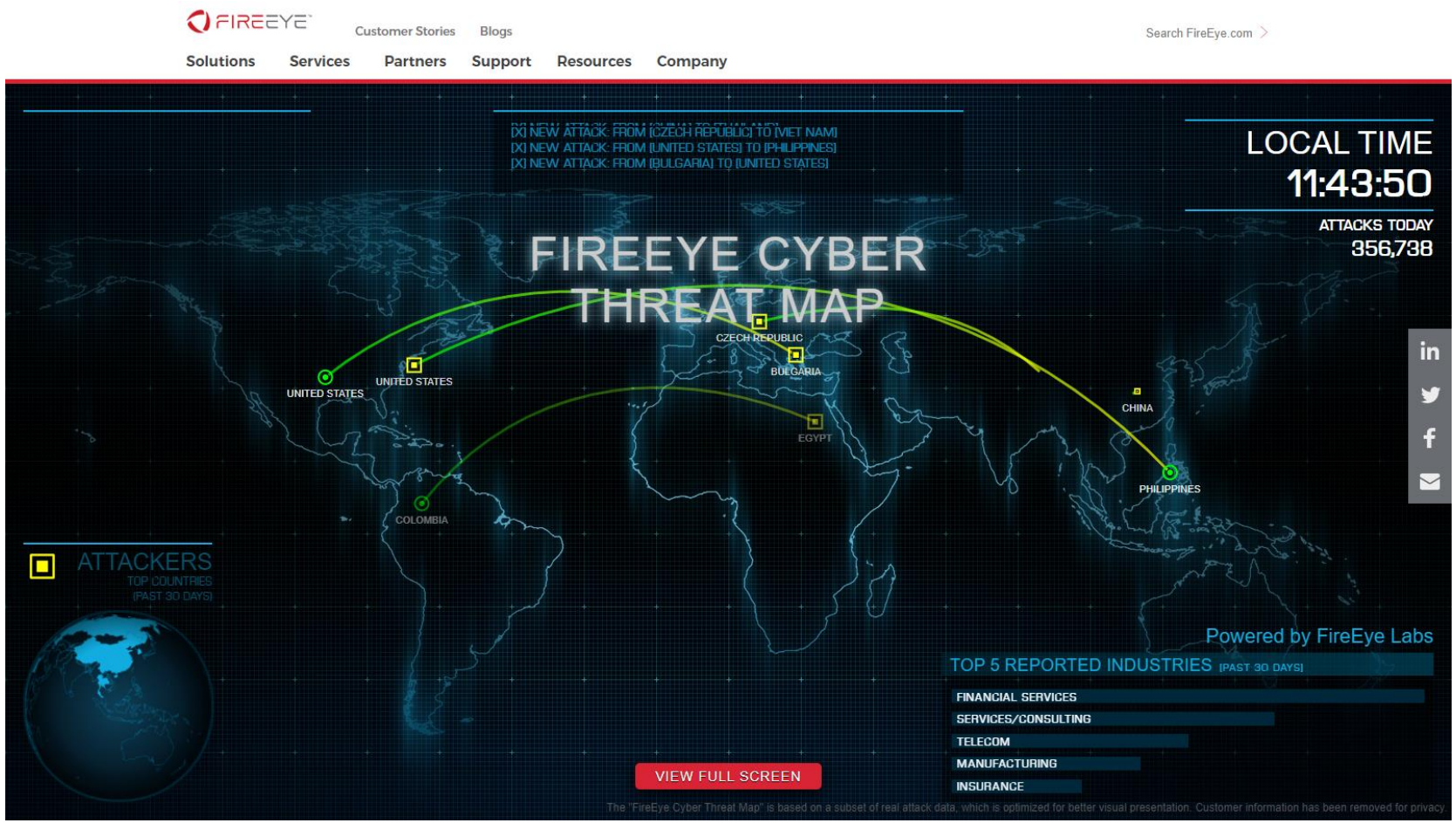
Indicators of compromise (IoCs) are just as the name suggests: indications that a system has been compromised by unauthorized activity. a common set of IoCs that firms should monitor include the following:

- Unusual outbound network traffic
- Anomalies in privileged user account activity
- Geographical irregularities in network traffic
- Account login red flags
- Increases in database read volumes
- HTML response sizes
- Large numbers of requests for the same file
- Mismatched port-application traffic, plain ports
- Suspicious registry or system file changes
- Unusual DNS requests
- Unexpected patching of systems
- Mobile device profile changes

Open Source Intelligence (OSINT)

Threat Maps

Threat maps are geographical representations of attacks showing where packets are coming from and going to



Vulnerability Management

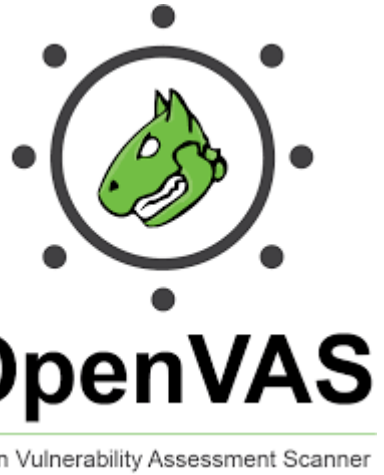
A vulnerability assessment seeks to identify issues in a network, application, database, or other IT systems prior to it being inadvertently or purposely used to compromise a system. Vulnerability assessments are a formalized process that define, identify, and classify the security holes in an enterprise network architecture

Vulnerability management is the practice of finding and mitigating the vulnerabilities in your computers in your networks.

Vulnerability Management

Tools for Vulnerability Assessments

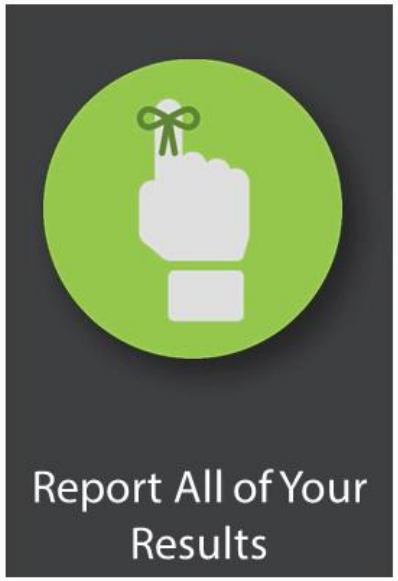
- Network Mapping **NMAP**
- Vulnerability Scanning **Nessus** , **OpenVAS**, **Nexpos** etc.
- Network Sniffing **Wireshark, TCPdump** and other
- Web application Vulnerability scanner
- Password Analysis tools



Ethical Hacking Defined:

Involves the Use of Hacking Methods and Tools to Discover Weaknesses for System Security

What Skills Should an Ethical Hacker Have?



Red Team Vs Blue Team

Types of Pen Tests

Black Box | Gray Box | White Box

Depends on Your Approach